You're Being Tracked Online; Go Tell Your Friends

Public involvement can be detrimental to finding solutions to certain problems. In the Cold War, the public enacting vigilante justice on suspected communists could have been very bad. During COVID-19, public participation was important for solving and mitigating the outbreaks. To accomplish this, the government ran public education campaigns throughout 2020 and 2021 to increase awareness. Online tracking is like COVID-19 in that public participation is necessary in solving it. Online tracking is a pervasive problem of modernity, and the affected populace must be informed of its possible consequences, because if they are not active participants, average internet users will surrender their privacy out of ignorance only. In this essay, I argue that the way experts talk about and try to find solutions for surveillance capitalism, specifically browser fingerprinting, should change to include public education because the public is affected by tracking every day and must make informed decisions about it.

At the core of this conversation is the reality that we live in an age of what Harvard Professor Shoshanna Zuboff called "surveillance capitalism." In her book, "The Age of Surveillance Capitalism," Zuboff defines this new kind of capitalism as businesses treating data about individuals as a commodity that isn't owned by the individual (1 III. 3). According to the book's explanation of twenty-first century life, "rights to privacy… have been usurped by a bold market venture powered by unilateral claims to others' experience" (Zuboff, 1 II. 2). In essence, surveillance capitalism means that a person's data is available to the highest bidder without the person's consent. This transition to a new type of economy where personal data is a public commodity is similar to the transition from small family farms to large scale industry that occurred in the late 19th century (1 V. 2). To clarify, industrialization changed the role of the individual in the same way that surveillance capitalism has the capability to (1V. 2). The

potential change in the relations between individuals and businesses could affect every person who uses the internet, which is why the new dangers of the online sphere need to be discussed and should be public knowledge.

The need for discussion on online tracking is my main reason for writing this essay. Zuboff's book shows there is an ongoing conversation about surveillance capitalism, and that conversation is mostly among experts and researchers. The conversation needs to be brought to the ordinary people who it affects. Essentially, the experts who are trying to stop surveillance capitalism should prioritize involving the public. The questions of the conversation are whether surveillance capitalism is a problem and, if it is, what should be done about it. Historically, society has sometimes chosen to simply accept a problem instead of trying to fix it. For example, consumerism simply became a part of American society, instead of people trying to go back to the old ways of individual production and thriftiness (American Consumerism). Due to this possibility, society must decide if surveillance capitalism is something that should be fixed or something that will just become a normal part of life.

What to do about surveillance capitalism is hard to answer democratically because, at the moment, experts, such as Zuboff and computer science researchers, including Pau et al., P. Laperdrix, and Iqbal et al. (who have been cited a combined 790 times). The experts have a consensus that a solution for the trend of decreased individual privacy is an "urgent need" (Pau et al. 1). In the big picture of this issue, experts agree about nearly everything except how the issue should be solved. On the other hand, average people, like Jacob Roach, who wrote a *Wired* article about online tracking, don't agree about whether the new methods of tracking even need a solution. Roach states that if someone doesn't want their information sold, they shouldn't be online (Roach). This idea is common sense to most people, but Roach has never been cited and is

not involved in the academic discussion on online tracking. Because of this potential blind spot for experts in what the public is actually willing to do about their privacy, it is important that the experts on this issue not only try to find solutions with their own studies but also inform the public. As Pau et al. say, making research on the subject publicly available will be necessary for further research to gain traction and for the problem to eventually be stopped (14).

An issue from the expert's perspective is that, once the public is involved, there is a possibility that many people will take the approach Roach does. This approach is to simply choose not to invest resources into stopping the rise of surveillance capitalism; if enough people choose to do this, society as a whole won't make a significant enough effort. At this point, you are probably asking why society needs to make an effort, why surveillance capitalism is a problem at all. There are many things that companies may do with an individual's data: from producing targeted ads to assessing the risk of providing insurance. Some people may not care about these things, but some people do – and the people who do care need to know about the issue.

The crux of my argument is that even if many people may not care, the public should still be informed of the consequences of surveillance capitalism, because the choice between privacy and convenience should be conscious. Foucault said, "freedom may well appear as the condition for the exercise of power," or in simpler terms, individuals have to choose to surrender control for companies to have true control over them (12). Foucault's work has been cited over 27,000 times, and his work on the idea of freedom and information is critical to understanding the deeper philosophical reasons why surveillance capitalism is an issue. Most people don't know the consequences of allowing surveillance capitalism, and it's problematic if individuals have enough freedom to cause a problem but lack knowledge of the consequences. This gap in

knowledge is ominous because it means that society is giving business more control, which is only fine if that is what we knowingly choose to do.

Because individuals need to have knowledge of the consequences of decreased online privacy and must be involved if there is to be major progress towards a solution, spreading awareness of the problem is the next major step. The research into surveillance capitalism does not say it is some existentialist threat, but that it is still something people need to know about (Lawall 7). Surveillance capitalism is a threat because, as technologies for tracking have developed, people's knowledge hasn't kept up (Faiz Khamedi 1).

Tracking used to be mostly accomplished through browser cookies, something most people know about (Iqbal 1). Unfortunately, websites can now use a new method of "stateless" tracking that is very difficult to detect (Iqbal 2). Stateless tracking is when the method of tracking doesn't rely on the user's hardware and can't be stopped by normal safeguards, making it much more secretive and enabling businesses to secretly obtain users' information (Iqbal 2). This method is called "browser fingerprinting" and tracks users via the combination of unique aspects of their system, such as operating system and time zone (Pau 9). For example, if your computer is running Linux, in the Eastern American time zone, with English set as the main language, and a certain screen resolution, you are probably very close to unique and can be tracked across many websites (Pau 9). The issue with this is that "even when cookies are disabled, fingerprints can be used to fully or partially identify users or devices" (Pau 1). Individuals can find out if their system is unique (and therefore trackable) at Amiunique.org, but most people don't go to the trouble (Laperdrix 1).

Many people don't know about this new tracking technology (Faiz Khademi 1) and therefore surrender their privacy to surveillance capitalism with the click of a button (Zuboff 1 II.

2). The button that surrenders your information is the one at the end of the terms and conditions that usually go unread (Zudoff 1 II. 2). For example, to be fully informed about the terms and conditions for Google's smart home device, Nest, one would "need to review nearly a thousand … contracts" which most people don't have time for (Zudoff 1 II. 2). So most people allow companies to track them, something that is problematic because they likely don't fully understand the consequences of their actions.

There is a second implication of fingerprinting that shows how pervasive surveillance capitalism is. According to researcher Alexander Lawall, cookies require permission to access a user's data, but "fingerprinting does not require such consent" (1). Additionally, a study by Iqbal et al. used new ways to track browser fingerprinting and found code for hidden tracking of users across "2349 different domains" (14). New technologies have made surveillance capitalism even more powerful, and awareness of the extent of the consequences is now even more important.

The experts in this field have mostly focused on direct solutions instead of raising awareness. One attempted solution to the dangers of surveillance capitalism is using new methods of detection, such as those developed by Iqbal et al. and Pau et al. These are useful because "Most of the browser fingerprinting tools are … in a form that has never been made public" (Pau 2). Even so, "[Academics] … have long struggled to provide meaningful protections against browser fingerprinting" (Iqbal et al. 1). Browser fingerprinting is hard to detect and even harder to prevent, so these new dangers to privacy can't really be stopped by experts (Pau 2). Therefore, to reference my example in the beginning, the problem of surveillance capitalism is more of a COVID-19 problem than a Cold War one, and the most important thing is increased awareness.

Because most experts are against surveillance capitalism, but most internet users are complacent (likely out of accidental ignorance), there hasn't been much progress in stopping surveillance capitalism. Notably, "It is possible to improve privacy and anonymity on the web while still retaining a modern and comfortable web experience" (Laperdrix 1). However, because of the lack of public support for fighting browser fingerprinting and other tools of surveillance capitalism, most solutions are only from one end (and not the user's end) (Lawall 7). By necessity, "The majority of solutions just aim to reduce the likelihood of obtaining a browser fingerprint" instead of stopping it outright (Pau 1).

If universities and experts in computer science want to continue to invest resources towards stopping surveillance capitalism, they need the support of the greater population (Lawall 7). If they don't have broad public support, then their solutions won't be effective because they will only be implemented partially (Lawall 7). If the greater population is apathetic to the problem, then the efforts of these experts should be focused elsewhere because they would not be useful without public support. Moreover, the apathy of the general populace should only be considered as a variable in the conversation if it is a purposeful choice to indulge surveillance capitalism and not one made out of ignorance.

So that society has the knowledge to justify the freedom that is the "condition for the exercise of power," you should tell your friends about browser fingerprinting and the new dangers of surveillance capitalism (Foucault 12). Whether or not you care about your privacy, you should inform yourself and others about the new online dangers we face every day. If enough people do so, the choices society makes about allowing the use of data by companies will be purposeful and not out of ignorance. So, while this essay is a call to action, it is one promoting education about the problem and not a certain solution for that problem.

Works Cited

Derrida, Jacques. *Of Grammatology.* Johns Hopkins University Press, 1976. Translated by Gayatri Spivak.

Faiz Khademi, Amin. "Browser Fingerprinting: Analysis, Detection, and Prevention at Runtime." 2014. ProQuest Dissertations & Theses. https://unr.primo.exlibrisgroup.com/permalink/01UNR_INST/adtd5q/cdi_proquest_journals_1823609464

Foucault, Michel. "The Subject and Power." In Beyond Structuralism and Hermeneutics, edited by H. Dreyfus and P. Rabinow, 208-226. The University of Chicago Press, 1983. https://foucault.info/documents/foucault.power/

Knight Foundation. *Thinking Strategically About Informing the Public on Complex Issues*. Amazon S3, 2017.

Laperdrix, P., Rudametkin, W., and Baudry, B., "Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 878-894, https://ieeexplore.ieee.org/document/7546540.

Lawall, Alexander. "Fingerprinting and Tracing Shadows: The Development and Impact of Browser Fingerprinting on Digital Privacy." arXiv.org, 2024. https://unr.primo.exlibrisgroup.com/permalink/01UNR_INST/adtd5q/cdi_proquest_journals_3130963951

Iqbal, Umar, et al. "Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors." Proceedings - IEEE Symposium on Security and Privacy, IEEE, 2021, pp. 1143–61, https://doi.org/10.1109/SP40001.2021.00017.

Pau, Kiu Nai, et al. "The Development of a Data Collection and Browser Fingerprinting System." Sensors (14248220), vol. 23, no. 6, Mar. 2023, p. 3087. EBSCOhost, https://doi-org.unr.idm.oclc.org/10.3390/s23063087.

Roach, Jacob. "Here's What Your Browser Is Telling Everyone About You." Wired, 16 October 2025, https://www.wired.com/story/what-is-browser-fingerprinting/.Accessed. Accessed 17 November 2025.

"The rise of American Consumerism." PBS.org, https://www.pbs.org/wgbh/americanexperience/features/tupperware-consumer/. Accessed 9 January 2026.

Zuboff, Shoshana. *The Age of Surveillance Capitalism*. Profile Books, 2019.